



Sécurité offensive

## Techniques de hacking - Niveau 1

5 jours (35h00) | ★★★★★ 5/5 | SEC-HACK | Évaluation qualitative de fin de stage |

Formation délivrée en présentiel ou distanciel

Formations Informatique > Cybersécurité > Sécurité offensive

Document mis à jour le 30/05/2023

### Objectifs pédagogiques

- Détecter les fragilités d'un système par la connaissance des différentes cibles d'un piratage
- Appliquer des mesures et des règles basiques pour lutter contre le hacking
- Identifier le mécanisme des principales attaques.

### Modalités et moyens pédagogiques

Formation délivrée en présentiel ou distanciel\* (e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatique...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Niveau requis

Posséder des bases dans la sécurité des systèmes d'information. Connaître le fonctionnement d'un réseau, maîtriser des connaissances dans la gestion des données et de leur circulation.

### Public concerné

Décideurs, responsables DSI, responsables sécurité du SI, chefs de projets IT.

## **Cette formation :**

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

# **Programme**

## **Jour 1**

### **Introduction : les fondamentaux**

- L'histoire et la nomenclature
- La veille en cybersécurité
  - Liens
  - Plateformes
  - Analyse
- Organisation des acquis
  - MindMap
  - Notion
  - Start.me
- Découvrir les principaux types d'attaques
- Les différentes phases d'une attaque (Kill Chain)

### **Découvrir la notion de vulnérabilité**

- Les standards de gestion de vulnérabilités
  - CVE, CVSS, MITRE, CWE, NVD, IOC, OTX, Exploit, TTP
- Découvrir le framework ATT&CK
- Déploiement d'une plateforme de simulation pentest
- La récolte d'information :
  - Récolte passive
  - Récolte active

## **Jour 2**

### **La récolte passive**

- IP
- DNS
- Localisation
- Dorks
- CSE
- Collecte de renseignements
- Créer sa légende
- Osint
- Socmint
- Humint
- Fuites de données
- Add-ons
- Cryptomonnaie
- OSINT framework
- Sleuthing

### **Exemple de travaux pratiques (à titre indicatif)**

- Utiliser les techniques de recherche passive pour collecter des informations

## **Jour 3**

### **La récolte active**

- Nmap, Hping3, Netdiscover, OS Fingerprinting, Banner grabbing
- Recherches de vulnérabilités
- Evaluation des vulnérabilités
- Les frameworks
- Les sites

### **Exemples de travaux pratiques (à titre indicatif)**

- Utiliser les outils de scanning
- Utiliser les outils de recherches de vulnérabilités

## **Jour 4**

### **L'exploitation**

- Metasploit
  - Architecture, interfaces, modules, exploits, payloads, Meterpreter shell
- L'exploitation de vulnérabilité avec Metasploit
- Payload-generation

### **Exemple de travaux pratiques (à titre indicatif)**

- Utiliser Metasploit

## **Jour 5**

### **MITM (Man-In-The-Middle)**

- Principes et techniques
- MAC flooding, ARP poisoning, DNS spoofing...

### **Brute Force (attaque par force brute)**

- Principes et techniques
- Dictionnaire, hybride, credential stuffing

### **Exemples de travaux pratiques (à titre indicatif)**

- MITM et Brute Force

### **Contre-mesures**

- Organisationnelles et techniques

### **Examen M2i (en option)**

- Prévoir l'achat de l'examen en supplément
- L'examen (en français) sera passé le dernier jour, à l'issue de la formation et s'effectuera en ligne
- Il s'agit d'un QCM dont la durée moyenne est d'1h30 et dont le score obtenu attestera d'un niveau de compétence
- L'examen n'est pas éligible au CPF, mais permettra néanmoins de valider vos acquis

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

## **Modalités d'évaluation des acquis**

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation et/ou un examen M2i

## **Les + de la formation**

Un examen M2i permettant de valider vos acquis à l'issue de la formation est disponible sur demande (coût : 120€).